CLAIMS

We claim

1. A cryptographic key server suitable for providing cryptographic services to remote devices coupled to said cryptographic key server via a network, said cryptographic key server comprising:

a secure network interface engine executing on said cryptographic key server, said secure network interface engine operable:

to establish a secure network communication channel with at least one remote device;

to unmarshal secured cryptographic service requests received from said at least one remote device; and

to marshal and transmit secure cryptographic service responses to said at least one remote device; and

a cryptographic service engine executing on said cryptographic key server, said cryptographic service engine being in bi-directional communication with said secure network interface engine, said cryptographic service engine operable to provide cryptographic services requested by said at least one remote device via said secure network interface engine.

2. The cryptographic key server as recited in Claim 1, wherein said at least one device is an application server.

3. The cryptographic key server as recited in Claim 1, wherein said secure network interface engine is arranged such that said secure network communication channel is established according to a Secure Socket Layer (SSL) protocol.

4. The cryptographic key server as recited in Claim 1, wherein said secure network interface engine is arranged such that said secure network communication channel is established according to a Transport Layer Security (TLS) protocol.

5. The cryptographic key server as recited in Claim 1, wherein said secure network interface engine supports multiple communications protocols including a Secure Socket Layer (SSL) protocol and a Transport Layer Security (TLS) protocol, said secure network interface engine being responsive to said at least one device to establish said secure network communication channel according to a protocol selected by said at least one device.

6. The cryptographic key server as recited in Claim 1, wherein said cryptographic service engine and said secure network interface engine are components of a single process executing on said cryptographic key server.

7. The cryptographic key server as recited in Claim 1, wherein said cryptographic service engine is operable to perform encryption and decryption functions.

8. The cryptographic key server as recited in Claim 7, wherein said encryption and decryption functions comprise:

symmetric block ciphers;

generic cipher modes;

stream cipher modes;

public-key cryptography;

padding schemes for public-key systems;

key agreement schemes;

elliptic curve cryptography;

one-way hash functions;

message authentication codes;

cipher constructions based on hash functions;

pseudo random number generators;

password based key derivation functions;

Shamir's secret sharing scheme and Rabin's information dispersal algorithm (IDA);

DEFLATE (RFC 1951) compression/decompression with gzip (RFC 1952) and zlib (RFC 1950) format support;

fast multi-precision integer (bignum) and polynomial operations;

finite field arithmetic, including GF(p) and GF(2^n); and

prime number generation and verification.

9. The cryptographic key server as recited in Claim 7, wherein said encryption and decryption functions comprise:

DES, 3DES, AES, RSA, DSA, ECC, RC6, MARS, Twofish, Serpent, CAST-256, DESX, RC2, RC5, Blowfish, Diamond2, TEA, SAFER, 3-WAY, Gost, SHARK, CAST-128, Square, Shipjack, ECB, CBC, CTS, CFB, OFB, counter mode(CTR), Panama, ARC4, SEAL, WAKE, Wake-OFB, Blumblumshub, ElGamal, Nyberg-Rueppel (NR), Rabin, Rabin-Williams (RW), LUC, LUCELG, DLIES (variants of DHAES), ESIGN padding schemes for public-key systems: PKCS#1 v2.0, OAEP, PSSR, IEE P1363 EMSA2, Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), LUCDIF, XTR-DH, ECDSA, ECNR, ECIES, ECDH, ECMQV, SHA1, MD2, MD4, MD5, HAVAL, RIPEMD-160, Tiger, SHA-2 (SHA-256, SHA-384, and SHA-512), Panama, MD5-MAC, HMAC, XOR-MAC, CBC-MAC, DMAC, Luby-Rackoff, MDC, ANSI X9.17 appendix C, PGP's RandPool, PBKDF1 and PBKDF2 from PKCS #5.

10. The cryptographic key server as recited in Claim 1, wherein said cryptographic service engine is operable to perform signing and verifying functions.

11. The cryptographic key server as recited in Claim 10, wherein said signing and verifying operations includes RSA and DSA.

12. The cryptographic key server as recited in Claim 1, wherein said cryptographic service engine is operable to perform hashing operations.

13. The cryptographic key server as recited in Claim 10, wherein said hashing operations includes HMAC with SHA-1.

14. The cryptographic key server as recited in Claim 1, wherein said cryptographic service engine is further operable to authenticate and to determine authorization of a request for cryptographic services prior to and as a condition of performing said cryptographic services.

15. The cryptographic key server as recited in Claim 14, wherein authenticating a request for cryptographic services includes verifying an identity of one or more of a set comprising:

a client that is requesting for cryptographic services;

said at least one remote device from which said client requesting for cryptographic services;

a function or program that is executing on said at least one remote device.

16. The cryptographic key server as recited in Claim 14, wherein determining authorization of a request for cryptographic services includes determining authorization privileges granted to one or more of a set comprising:

a client that is requesting for cryptographic services;

said at least one remote device from which said client requesting for cryptographic services;

a function or program that is executing on said at least one remote device.

17. The cryptographic key server as recited in Claim 16, wherein the operation of determining authorization a request for cryptographic services further includes determining whether said request for cryptographic services is within the privileges of a requestor that is associated with said request for cryptographic services.

18. The cryptographic key server as recited in Claim 1, wherein said cryptographic service engine is operable to track requests for cryptographic services.

19. The cryptographic key server as recited in Claim 1, said cryptographic key server further comprising:

a private key engine, said private key engine operable to provide private keys for use by said cryptographic service engine in performing cryptographic services.

20. The cryptographic key server as recited in Claim 1, wherein said cryptographic key server is a network security appliance.

21. The cryptographic key server as recited in Claim 1, wherein said cryptographic key server has a computer hardware architecture supporting said cryptographic service engine and said secure network interface engine, said computer hardware architecture comprising:

a databus;

a central processing unit bi-directionally coupled to said databus;

a persistent storage device bi-directionally coupled to said databus;

a transient storage device bi-directionally coupled to said databus;

a network I/O device bi-directionally coupled to said databus;

a cryptographic accelerator card bi-directionally coupled to said databus;

a hardware security module bi-directionally coupled to said databus and suitable for storing private keys; and

a smart card interface device.

22. The cryptographic key server as recited in Claim 21, wherein said hardware security module is a tamper resistant device.

23. The cryptographic key server as recited in Claim 21, wherein said private keys are loaded into said hardware security module and stored in an encrypted format.

24. The cryptographic key server as recited in Claim 21, wherein said private keys are loaded into said hardware security module via a smart card storing said encrypted private keys.

25. The cryptographic key server as recited in Claim 24, wherein said cryptographic key server supports a k-out-of-n secret sharing such that said private keys may only be accessed by said cryptographic key server after k smart cards have been inserted.

26. A cryptographic key server suitable for providing cryptographic services to remote devices coupled to said cryptographic key server via a network, said cryptographic key server comprising:

a cryptographic accelerator card bi-directionally coupled to a databus;

a smart card interface device;

a hardware security module bi-directionally coupled to said databus and suitable for secure data; and

and wherein said secure data is accessible only when k-out-of-n smart cards are inserted into said smart card interface device.

27. An application server capable of hosting a plurality of applications, said application server operable for providing services to a plurality of clients via a network, said application server comprising:

a cryptographic application program interface (API), said cryptographic API providing a set of standards by which said plurality of applications can invoke a plurality of cryptographic services, at least one of said plurality of cryptographic services being performed by a remote cryptographic key server; and

a secure network interface engine, said secure network interface engine operable to establish a secure network communication channel with the remote cryptographic key server.

28. The application server as recited in Claim 27, wherein said cryptographic API is operable to utilize said secure network interface engine to request remote cryptographic services.

29. The application server as recited in Claim 27, wherein said cryptographic API is exposed as Java Cryptography Extensions (JCE) to said plurality of applications.

30. The application server as recited in Claim 27, wherein said cryptographic API is exposed via Cryptographic Service Provider (CSP) and said cryptographic API is implemented as a Dynamic Linked Library.

31. The application server as recited in Claim 27, wherein said cryptographic API is exposed via MS-CAPI.

32. A device capable of executing a plurality of functions and programs, said device comprising:

a secure network interface engine executing on said device, said secure network interface engine operable to establish a secure network communication channel with at least one remote cryptographic key server, marshal and transmit secure requests for cryptographic services to said at least one remote cryptographic key server, and receive and unmarshal secure responses to requests for cryptographic services; and

a cryptographic application program interface (API) executing on said device and bi-directionally coupled with said secure network interface engine, said cryptographic API providing a set of standards by which said plurality of functions and programs can call a corresponding plurality of cryptographic services, wherein at least one of said plurality of cryptographic services is performed remotely by said at least one cryptographic key server, said cryptographic API being responsive to a request for said at least one remote cryptographic service to utilize the secure network interface engine to request said cryptographic services.

33. A computer-implemented method for providing cryptographic key services, said method comprising the acts of:

establishing a set of private keys on a networked key server;

establishing a secure network communications channel between a networked device and said networked key server;

receiving a request for cryptographic key services at said networked key server from said networked device via said secure network communications channel;

authenticating said request for cryptographic key services;

determining authorization said request for cryptographic key services; and

performing said request for cryptographic key services at said networked key server utilizing said private keys when said request is authorized.

34. The computer-implemented method for providing cryptographic key services as recited in Claim 33, wherein said act of establishing private keys on a networked server includes the act of encrypting said set of private keys.

35. The computer-implemented method for providing cryptographic key services as recited in Claim 33, wherein said act of encrypting said set of private keys is done using a k-out-of-n secret sharing technique.

36. The computer-implemented method for providing cryptographic key services as recited in Claim 33, wherein said act of establishing a secure network communications channel includes use of a SSL protocol.

37. The computer-implemented method for providing cryptographic key services as recited in Claim 33, wherein said act of establishing a secure network communications channel includes use of a TLS protocol.

38. The computer-implemented method for providing cryptographic key services as recited in Claim 33, wherein said act of authenticating said request includes the act of authenticating an identity of one or more of a set comprising:

a client that is requesting for cryptographic services;

said networked device from which said client is requesting for cryptographic services; and

a function or program that is executing on said networked device.

39. The computer-implemented method for providing cryptographic key services as recited in Claim 33, wherein said act of determining authorization said request includes the act of determining authorization privileges granted to one or more of a set comprising:

a client that is requesting for cryptographic services;

said networked device from which said client is requesting for cryptographic services; and

a function or program that is executing on said networked device.

40. The computer-implemented method as recited in Claim 38, wherein the act of determining authorization said request includes the act of determining whether said request is within rights of a requestor that is associated with said request for cryptographic services.

41. The computer-implemented method as recited in Claim 33, further comprising the act of tracking all requests for cryptographic services.

42. A computer-implemented method for providing networked cryptographic key services, said method comprising the acts of:

integrating a cryptographic API within an application server;

exposing cryptographic services to a plurality of applications executing on said application server via said cryptographic API;

establishing a secure network communications channel between said application server and a remote cryptographic key server;

receiving a request for cryptographic services from an application at said cryptographic API;

marshalling said request for cryptographic services for transmission to said cryptographic key server;

transmitting said marshaled request for cryptographic services to said cryptographic key server via said secure network communications channel;

receiving a response to said request via said secure network communications channel;

unmarshalling said response; and

providing a usable response to said requesting application via said cryptographic API.

43. A method for securing cryptographic keys within a server system, the method comprising the computer-implemented acts of:

storing on a key server cryptographic keys used for encrypting data ; and

wherein said key server communicates with at least one component of said server system using a secure communications channel.

44. A method for securing cryptographic keys within a network system, the method comprising the computer-implemented acts of:

storing cryptographic keys used for encrypting data on a key server, and

wherein said key server is a dedicated network appliance that performs cryptographic operations on behalf of at least one component of said network system.

45. The method as recited in Claim 44, wherein said cryptographic operations include operations under a Secure Socket Layer (SSL) protocol.

46. The method as recited in Claim 44, wherein said cryptographic operations include operations under a Transport Layer Security (TLS) protocol.

47. The method as recited in Claim 44, wherein sensitive data is stored in said network system only in encrypted form.

48. A cryptographic key server appliance for securing cryptographic keys within a network system, wherein said cryptographic key server stores cryptographic keys and controls access to said stored cryptographic keys.

49. The cryptographic key server appliance as recited in Claim 48, wherein said access includes using at least one of said stored cryptographic keys solely for encryption operations.

50. The cryptographic key server appliance as recited in Claim 48, wherein said access includes using at least one of said stored cryptographic keys solely for decryption operations.

51. A cryptographic appliance for securing sensitive information within a server system, comprising:

a data communications bus;

a central processing unit bi-directionally coupled to said data communications bus;

transient memory bi-directionally coupled to said data communications bus;

persistent memory bi-directionally coupled to said data communications bus;

a network I/O device bi-directionally coupled to said data communications bus;

a crypto-accelerator unit bi-directionally coupled to said data communications bus;

a hardware security module; and

a smart card interface coupled to said data communications bus.

52. A computer-implemented method for providing cryptographic services in a network system, said computer-implemented process comprising the acts of:

securely loading cryptographic keys onto a key server;

establishing a secure transport session between a first component of said network system and said key server;

authenticating one or more components of said network including said first component to said key server;

determining authorization of said one or more components of said network including said first component to said key server;

making a request for cryptographic operations from said first component to said key server;

determining whether said request is to be performed by said key server based on results associated with the acts of authenticating and determining authorization;

if said request is authorized, then performing said requested cryptographic operations on said key server; and

providing the results of said requested cryptographic operations from said key server to said first component via said secure transport session.

53. A method for protecting data in a network system, said computer-implemented method comprising the acts of:

providing a network device for intercepting and inspecting data that is en route to an application server, wherein said network device is part of a pre-defined group of cryptographic servers that share a group key and said network device is operable for:

determining whether said data is sensitive data;

encrypting said data to form encrypted data if said data is sensitive, wherein the act of encrypting includes using a group key that is shared by said pre-defined group of cryptographic servers; and

forwarding said encrypted data to said application server;

storing said encrypted data in a storage medium associated with said application server; and

allowing one or more back-end application servers to employ one of said pre-defined group of cryptographic servers to retrieve said encrypted data from said storage medium and decrypt said encrypted data if said one or more back-end application servers is authorized to access said data.